無線LAN製品ご使用時におけるセキュリティに関するご注意
（お客様の権利（プライバシー保護）に関する重要な事項です！）

無線LANでは、LANケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由にLAN接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- ● 通信内容を盗み見られる
- 悪意ある第三者が、電波を故意に傍受し、IDやパスワード又はクレジットカード番号等の個人情報、メールの内容等の通信内容を盗み見られる可能性があります。

- ● 不正に侵入される
- 悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）
- などの行為をされてしまう可能性があります。

本来、無線LANカードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線LAN製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

無線LAN機器は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。
従って、お客様がセキュリティ問題発生の可能性を少なくするためには、無線LANカードや無線LANアクセスポイントをご使用になる前に、必ず無線LAN機器のセキュリティに関する全ての設定をマニュアルにしたがって行ってください。
なお、無線LANの仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解の上、ご使用下さい。
セキュリティの設定などについて、お客様ご自分で対処できない場合には、「BUFFALOサポートセンター」までお問い合わせ下さい。

当社では、お客様がセキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

社団法人　電子情報技術産業協会（JEITA）
「無線LANのセキュリティに関するガイドライン」より

裏面もお読みください

BUFFALOの無線LANセキュリティに対する取り組みについて

BUFFALOではお客様がより快適でセキュアな無線LANを簡単にお使いいただける様に製品開発に取り組んでおります。BUFFALOの無線LAN　AirStationシリーズの無線LANセキュリティについてご説明いたします。

① 簡単接続設定システム「AirStation One-Touch Secure System（AOSS）」

- 「AirStation One-Touch Secure System(AOSS)」は、これまで暗号化キーの設定や入力で煩雑だった無線LANの接続設定を飛躍的に簡単にする新技術です。これを使用することで、ワンタッチでセキュアな無線LANネットワークに接続できます。暗号化方式は、標準的な「WEP」（64/128bitWEP）のほか、最新のセキュリティであるWPAにも採用されている「TKIP」、米国政府の標準暗号化方式として採用されている強固な「AES」に対応しており、「AOSS」がそれぞれの機器のセキュリティ機能レベルを判断して最適な暗号化方式に自動設定します。

② プライバシーセパレータ

- 無線パソコン間の通信を禁止する機能です。これを使用することで、同一のアクセスポイントに接続している無線パソコンのデータが見えなくなるため、プライバシーの保護が可能です。

③ 無線送信出力制限

- 無線の送信出力を変更する機能です。この数値を低くすると、無線の届く範囲が短くなるため、不要な電波漏れによる不正アクセスを防止できます。

④ Any接続拒否

- ESSID（SSID）を「Any」にすることで誰でも接続できてしまう「Any接続」を禁止する機能です。

⑤ 無線ESSID（SSID）ステルス機能

- アクセスポイントが周辺に通知するために発信するビーコン信号を停止する機能です。WindowsXPなどのビーコン信号を検知する機能を搭載している端末からESSID（SSID）を分からなくすることができます。